International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:4, No:2, 2010

A Novel Approach to Avoid Billing Attack on VOIP System

Narendra M. Shekokar, and Satish R. Devane

***Abstract*—**In a recent year usage of VoIP subscription has increased tremendously as compare to Public Switching Telephone System(PSTN). A VoIP subscriber would like to know the exact tariffs of the calls made using VoIP. As the usage increases, the rate of fraud is also increases, causing users complain about excess billing. This in turn hampers the growth of VoIP .This paper describe the common frauds and attack on VoIP based system and make an attempt to solve the billing attack by creating secured channel between caller and callee.

***Abstract*—**VoIP, Billing-fraud, SSL/TLS, MITM, Replay-attack.

I. Introduction

VOICE over Internet Protocol (Voice over IP or VoIP) allows users to make phone calls over the internet. VoIP is accepted by mass because communication on VoIP network is more economical than traditional PSTN system. VoIP systems allow transmission of voice and data on the same network and it also support value added services such as conferencing, web collaboration and online gaming [1]. Billing on VoIP system is based on the transmission of the packets and not on the time factor as used in traditional telephone services. VoIP subscribers are always looking for exact bill for the call and add on services which they have subscribed. VoIP billing is based on VoIP signaling. Session Initiation Protocol (SIP)[2] is the dominant VoIP signaling protocol is proposed by Internet Engineer Task Force (IETF). H.323 [3] is another signaling protocol, which is proposed by International Telecommunication Union. These signaling protocols are responsible for establishing, maintaining and terminating the call, to locate users, and to control the media transport.

SIP based VoIP system is susceptible to confidentiality, integrity, availability threat. In this paper we have discussed four types of billing attack on VoIP system e.g. Invite Replay, Fake Busy, Bye Delay and Bye Drop attacks and also provided the solution that these attacks could not take place. In invite reply attack, attacker makes unauthorized calls by replaying intercepted INVITE messages. In fake busy attack, attacker hijacks VoIP calls of targeted VoIP subscriber and controls the VoIP call duration.

In bye delay attack attacker prolong the duration of established calls between targeted VoIP subscribers by delaying the BYE message and bye drop attack prolongs the duration of established calls between targeted VoIP subscribers by simply dropping the BYE messages [4].Above discussed attacks could either make calls without subscriber's authorization or prolong the duration of subscriber's call transparently.

We have made attempt to avoid billing fraud, by proposing mitigation technique using SSL/TLS, which establishes secured channel between caller and callee.

Our paper is organized as below. In section II, we have discussed the overview of SIP protocol. In section III we introduce billing attacks on VoIP system. Then we have proposed a solution to avoid the billing attacks in section IV. Finally, we have concluded the paper in section V.

II. Overview of SIP

SIP(Session Initiation Protocol) is an application layer signaling protocol specified by the IETF. SIP is text based protocol which is responsible for creation, modification or termination of the multimedia session. SIP protocol is more popular than the H.323 protocols because of its simplicity and flexibility. The SIP based VoIP system contains following components 1) User Agent (UA): It represents VoIP phones or End Points2) Proxy server: It acts on the behalf of UA and forwards the SIP messages to its destination. 3) Redirect server: A redirect server receive a request from UA and informs about the next hops server.4) Registrar server & location server: These servers handles the UA's registration request and maintain database, which contain information about the location and user preferences as indicated by the UA.

Once session is established, UA sends RTP voice stream to each other based on negotiated media session parameter. At the end of the call caller first hangs up first and then send BYE message to its peer. Vulnerabilities found in SIP based authentication is listed as below [4].

- SIP authentication is applied to a few SIP messages (e.g., INVITE, BYE, REGISTER), and it leaves other important SIP messages (e.g., TRYING, RINGING, 200 OK, ACK and BUSY) unprotected.
- SIP authentication protects a few SIP fields (e.g., URL, username, realm), and it leaves other important SIP fields (e.g., SDP, From, To) in unprotected format.
- Authentication is applies to SIP messages from the UA (i.e., SIP phone) to SIP servers, and it leaves all the SIP messages from the SIP servers to UA unprotected.

N. M. Shekokar is with Department of Computer Engineering, D. J. Sanghvi College of Engineering, Mumbai, India (e-mail: nshekokar@yahoo.co.in).
S. R. Devane is with Department of Computer Engineering, Ramrao Adik College of Engineering, Navi Mumbai, India (e-mail: satish@rait.ac.in).

III. Billing Threats

In this section, we have discussed four types of billing attack [4], which are result of SIP authentication vulnerability. This vulnerability allows man-in-the-middle (MITM) to exist between the SIP server and the SIP UA and allows modifying the fields which are not protected. MITM can intercept the SIP messages and replay it to establish unauthorized callx, it can also prolong the duration of call which is established between VoIP subscribers. Result of this is subscriber will charge for the call which he has not made.

A. InviteReplay Billing Attack

InviteReplay billing attack exploits the vulnerability of SIP authentication. This attack could be effective even if the INVITE messages are protected by SIP authentication. MITM can view and intercept all messages which are exchange between UA and Server. Fig. 1 shows exchange of messages between UA and Sever. Initial INVITE message is ignored by MITM because it does not contain enough credential information to carry out Replay attack. MITM intercept INVITE message with credential information and send it to the attacker, upon receiving the information then attacker can mount Replay billing attack by replaying modified INVITE message.

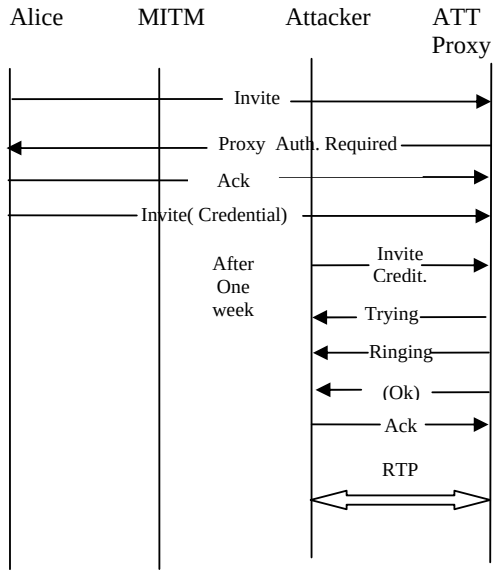

Fig. 1 Message flow of fake InviteReplay Billing attack

B. FakeBusy Billing Attack

In FakeBusy Billing attack, attacker hijacks the call between VoIP subscribers and prolongs the call duration. As a result, the call attempted by the VoIP subscriber would fail, and VoIP subscriber will be billed for the unauthorized call. As given in the following Fig. 2, two MITM exists between UA (Alice and Bob) and Server. MITM intercepts the INVITE message with credential information and send modified message to Vonage Server. This Server will forward the modified INVITE message to AT&T Server. Upon receiving the messages the AT&T Server will forward it to callee, before reaching it to the callee message is get intercepted by MITM2 and replies it replies back with messages (TRYING, RINGING, OK). This will allow MITM1 and MITM2 to exchange RTP stream till MITM2 is not generating BYE message. As a result of this caller is charged for unauthorized call.

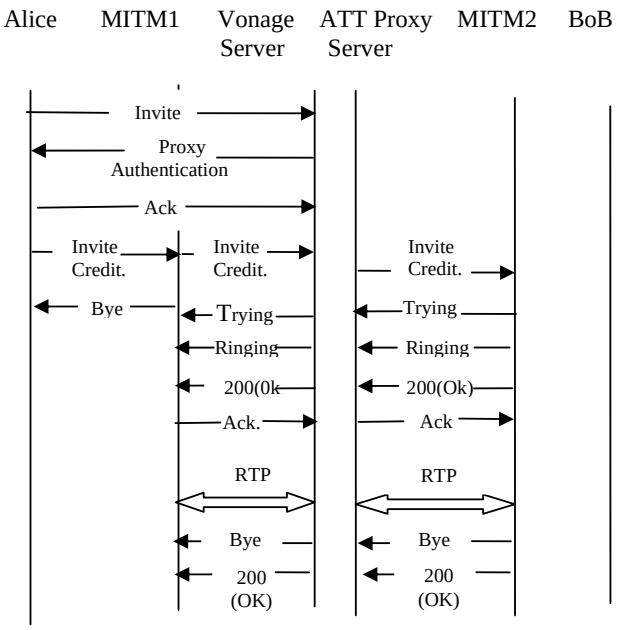

Fig. 2 Message flow of fake busy billing attack

C. ByeDelay Billing Attack

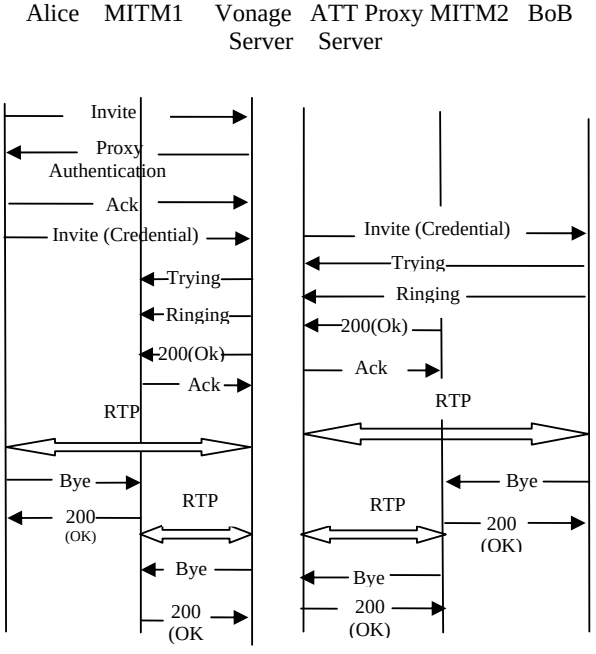

Fig. 3 Message flow of fake busy billing attack

ByeDelay billing attack prologs the call duration of established call between UA (Alice & Bob) by delaying BYE message, as mentions in Fig. 3, two MITM is exists between SIP phone and Server. After successful RTP streams exchange between caller and callee, the callee then sends BYE message to terminate the call. This BYE message is intercept by MITM and sends back 200 OK messages to callee and the caller respectively. The caller and callee is under impression that call is terminated while MITM's has establishes unauthorized call and exchange bogus RTP. This would give the service providers the impression that the caller and the callee are still actively talking, and gets charge for unauthorized call.

D. ByeDrop Billing Attack

Similar to ByeDelay billing attack, two MITMs is exits between SIP phones and server. As given in Fig. 4, MITMs intercept the BYE messages send by callee and replied it with 200 OK messages, as a result of this is the caller and callee is under impression that the call has been terminated successfully. This will allow MITMs to exchange bogus RTP streams about 20 minutes till the MITM2 does not stopped sending RTP streams. Surprisingly, both Vonage's RTP server and AT&T's RTP server keeps sending unidirectional RTP streams to Vonage phone and AT&T phone respectively for about 218 minutes. After replaying those RTP streams, we could find out that they were just background sounds. After about 218 minutes, the Vonage SIP server and AT&T SIP server sents the BYE messages to terminate the call. Fig. 4 shows message exchange in ByeDrop billing attack.

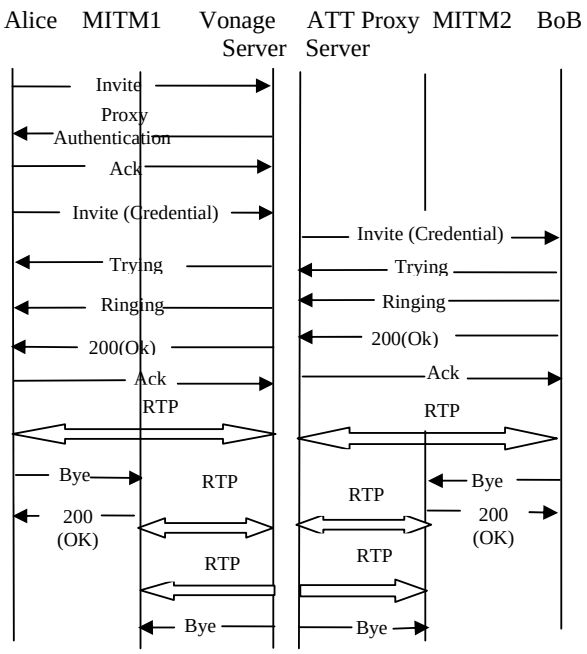

Fig. 4 Message flow of ByeDrop Billing attack

IV. Proposed Mitigation Technique of Billing Attack

There are two levels of security approach to defend the billing attack.

1 Hop-to-hop level Security: It established a secured communication link between two successive SIP entries in the path of signaling messages.

2 End-to-end Level Security: This security mechanism secured the communication between caller and callee. End-to-end security can be achieved by IPSec or SSL/TLS. IPSec is not used directly between two end points because it encrypt data between end-to-end, while SIP proxy server between SIP end points would not be able to interpret and modify required information in the SIP messages, which is lighter-weight and more easily managed protocol than IPSec, and thus more appropriate for SIP based VoIP system.[5] SSL operates between transport layer and application layer which support authentication and encrypted communication between SIP phone & server. It also maintains the integrity of messages.

The SSL contain three sub-protocols: 1) Handshake protocol 2) Record protocol 3) SSL alert protocol. [6]

1) Handshake protocol: It is responsible for initiating logical connection, caller and callee authentication and key exchange.

2) Record protocol: This protocol provides confidentiality and integrity to an SSL connection. Confidentiality is achieved by using the secret key which is define by handshake protocol while integrity is achieved by MAC.

3) SSL alert protocol: This protocol is responsible for detecting the error either at client side or server side. If error is fatal, both the party will immediately close the SSL connection.

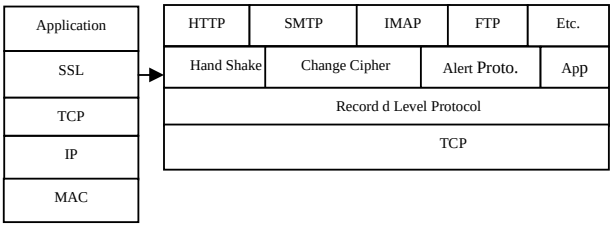

Fig. 5 SSL protocol Stack

An SSL session always begins with an exchange of message called an SSL handshake. As given in Figure 6 first UA(Alice, Bob) will register themselves with key exchange server. Then Alice will send client's SSL version number, cipher settings, randomly generated data, and other information to server, which is required to establish a SSL session with the Alice. Server also exchange similar information to Alice. Upon receiving it, Alice requests for Bob certificate to key exchange server, as a response key exchange server issues a requested certificate to Alice. This Certificate contain public key of Bob, which is use by Alice to send encrypted secret key. This key is use by Alice and Bob to exchange all future messages. Finally, Alice sends a separate (encrypted) message indicating that the

client portion of the handshake is finished. In response server sends a separate (encrypted) message indicating that the server portion of the handshake is finished [6][7]. Once SSL handshake is completed then SSL session will begin.

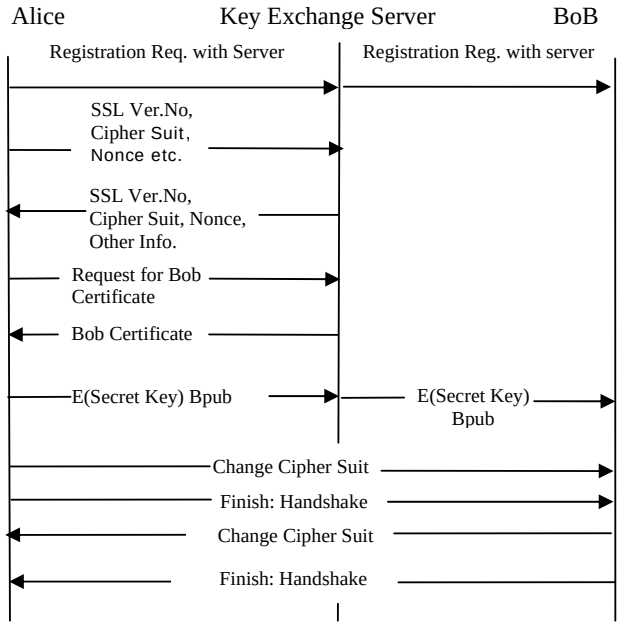

Fig. 6 SSL protocol message exchange

E. Avoidance Technique of InviteReplay Billing Attack

Once SSL/TLS connection is established between Alice and Server then VoIP session initialization, establishment is taking place using SIP protocol. Due to secured communication caller message is get exchange in encrypted format. In SIP session initialization, initial INVITE message is send by callee is rejected by server because it does not have essentials credit information to established SIP session with callee. Then once again Alice will send invite message with necessary credit information to the server. Like InvitReplay billing attack, MITM cannot observer and decrypt the intercepted invite message because message is sends in encrypted form and MITM does not hold secret key to decrypt it. Due to SSL/TLS secured cannel MITM is prevented to mount replay billing attack.

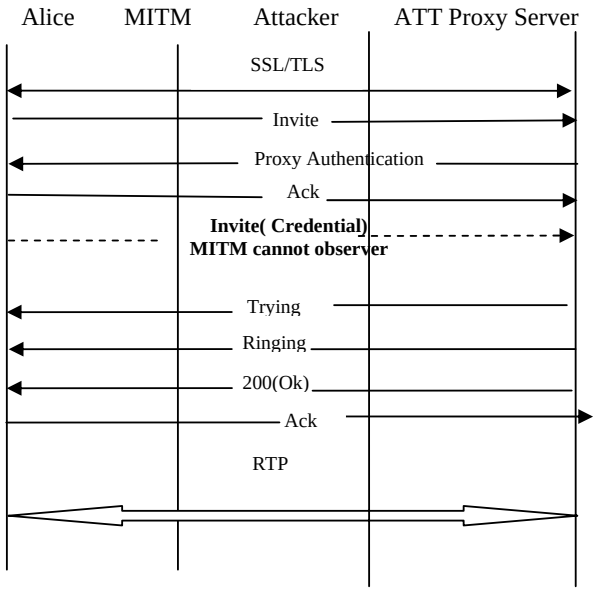

Fig. 7 Avoidance of InviteReplay attack using SSL/STL

F. Avoidance Technique of Fake Busy Billing Attack

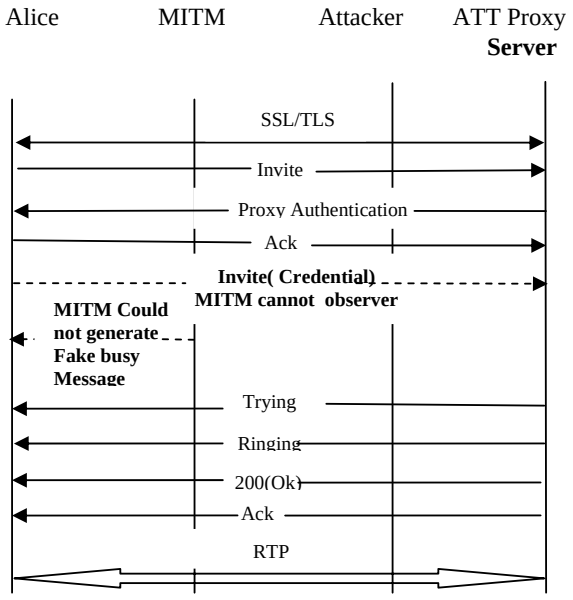

Fig. 8 Avoidance of FakeBusy Billing attack using SSL/TLS

Due to presence of SSL/TLS all the message is exchanged between client and Server in encrypted form, as a result of this MITM cannot observe and modify the INVITE message, it fails to collect the necessary information about Client. Hence, MITM is prevented from generating fake BUSY message to Alice and could not exchange bogus RTP stream between Client & Server.

Presence of SSL/TLS does not allow MITM to hijacks the call between Client and Server as well as prolongs the call

duration. As a result of this is Client will charge only for authorized call.

G. Avoidance Technique of Byedelay Billing Attack

Initial messages i.e Invite, Trying, Ringing, Ack, Ok exchange between Alice and Server is carried out via SSL/TLS. MITM forcibly cannot block or intercept these messages because of all message is send in encrypted for using secret key which is agreed by both party during SSL session. After this, caller and callee will exchange RTP stream. Finally, Alice will send BYE message to terminate the session. Like ByeDelay billing attack, this BYE message cannot be blocked by MITM because it is in encrypted form and it does not hold any secret key to decrypts it. MITM also prevented from exchanging bogus RTP stream with server. Due to secured channel Alice will charge for the authorized call.

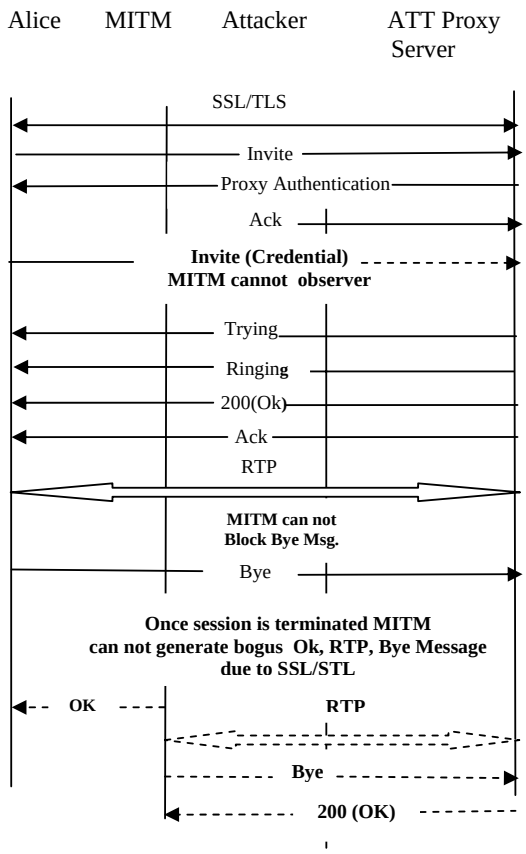

Fig. 9 Avoidance of ByeDelay Billing attack using SSL/STL

V. Conclusion

This paper has addressed in detailed threats of services on VoIP system. Here, we have discussed four types of billing attack: InviteReplay attack, FakeBusy attack, ByeDelay attack and ByeDrop attack on VoIP system. Any fraud in billing has direct impact on VoIP subscription. To avoid said frauds, we have attempted to propose a mitigation technique which established a secured channel using SSL/TLS. This channel provides a secured communication between caller and callee, it also maintain integrity of messages, authenticate caller and callee. First three billing attack is prevented using SSL/TLS, yet we have not address the mitigation technique of ByeDrop billing attack which will be future scope of our work.

References

[1] Rohit Dhamankar “Intrusion Prevention: The Future of VoIP Security”, [online].Available:http://www.tippingpoint.com/pdf/resources/whitepapers/503160-001_TheFutureofVoIPSecurity.pdf , 2004.

[2] J.Roshenburg et al., “SIP: Session Initiation Protocol”, IETF RFC 3261, June 2002.

[3] ITU, “Draft revised recommendation H323 V5”, Geneva, 20-30, May 2003.

[4] Ruishan Zhang, Xinyuan Wang, Xiaohui Yang, Xuxian Jiang, ”Billing Attacks on SIP-Based VoIP Systems”, Proceeding of the fIrst USENIX workshop on offensive Technology, August 06-10,2007.

[5] Secure SIP VoIP traffics,
[online].Available :http://www.techword.com/networking/features

[6] Atul Kahate,”Cryptography and Network Security”, 3rd Edition Tata McGraw-Hill ,2003.

[7] A draft on “Introduction to SSL”
[online].Available:http://docs.sun.com/source/816-6156-10/contents.htm,1998

[8] H. Abdelnur, V. Cridlig, R. State and O. Festor, “VoIP Security Assessment: Methods and Tools”, IEEE conference on VoIP MaSe 2006.

[9] Yanlan Ding, Guiping Su, “Intrusion detection system for signal based SIP attack through timed HCPN”, Second IEEE international Conference on Availability, Reliability, Security 2007.